UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/767,128	01/22/2001	Radia J. Perlman	P4098	2127

45774 7590 05/25/2006

KUDIRKA & JOBSE, LLP
ONE STATE STREET, SUITE 800
BOSTON, MA 02109

EXAMINER
CHEUNG, MARY DA ZHI WANG

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/767,128	PERLMAN, RADIA J.	
	Examiner	Art Unit	
	Mary Cheung	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) *12-16 and 21-27* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,17-20 and 28-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *1/30/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of the Claims

1. This action is in response to the amendment filed on March 15, 2006. Claims 1-37 are pending. Claims 12-16 and 21-27 are withdrawn. Claim 35 is amended. Claims 1-11, 17-20 and 28-37 are examined.

Response to Arguments

2. Applicant's arguments filed March 15, 2006 have been fully considered but they are not persuasive.

In response to the applicant's arguments that Kent (U. S. Patent 6,671,804) fails to teach a certificate includes a registration authority identifier, examiner believes that Kent teaches registration authority forwards a certificate request information to certification authority, wherein the certification request information comprising the identification information of the registration authority (column 9 line 32 – column 11 line 14); Kent further teaches a certificate includes specific authority information such as a specified authority or set of authorities (column 7 lines 1-62). It would have been obvious to one of ordinary skill in the art to allow the specific authority information in the certificate to include identifiers of authorities (i.e. the registration authority, certificate authority, attribute authority) for better protecting information from unauthorized usages. Thus, de Silva (U. S. Patent 6,564,320) modified by Kent as discussed in the office action teaches "...request includes a first identifier that identifies the registration authority; and at the certification authority in response to receipt of the request, generating a certificate that includes said first identifier".

In response to the applicant's arguments that the cited prior art fail to teach a time stamp associated with the request, examiner respectfully disagrees. De Silva teaches a time stamp that identifies expiration time (column 4 lines 65 – column 4 line 10). Kent teaches using time stamps to audit trails (column 11 lines 29-47). Since the purpose of time stamp is for tracking and recording time; thus, it would have been obvious to one of ordinary skill in the art to allow the time stamp in the teaching of de Silva modified by Kent to include a time associated with the request because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

In response to the applicant's arguments that the cited references fail to teach the limitations as claimed in claim 37, examiner believes that the limitations are taught by de Silva as revoking the compromised digital certificates (column 1 lines 11-15, 55-58 and column 4 line 65 – column 5 line 10).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 4-5, 6-11, 17-18, 20, and 34-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Silva et al., U. S. Patent 6,564,320 in view of Kent, U. S. Patent 6,671,804.

As to claim 1, de Silva teaches a method for certificate generation that enables efficient revocation of said certificate generated by an untrustworthy registration authority, comprising (abstract and column 4 line 65 – column 5 line 10):

At a the registration authority (local server 202 of Figs. 6-8):

- Receiving a request from a principal to issue a certificate on behalf of that principal (column 12 lines 3-12 and Figs. 6-8);
- Forwarding said request to a certification authority (column 12 lines 12-15 and Figs. 6-8);

At the certification authority (central server 104 of Figs. 6-8):

- In response to receipt of the request, generating a certificate (column 4 lines 44-58 and column 12 lines 15-19 and Figs. 6-8).

De Silva does not explicitly teach that the forwarded the certificate request includes a first identifier that identifies the registration authority, and the certificate is generated further includes said first identifier. However, Kent teaches the registration authority forwarding the certificate request includes the identifier of the registration authority (column 9 line 32 – column 10 lines 5 and Fig. 5), and if the identity of the registration authority is positively identified, generating a certificate (column 10 line 1 – column 11 line 14). Kent does not explicitly teach the generated certificate must include the identifier of the registration authority; however, Kent teaches the certificate includes specific authority information such as certificate authority, attribute authority, registration authority (column 7 lines 36-62). It would have been obvious to one of ordinary skill in the art to allow the certificate in Kent's teaching include the identity of the registration

authority for better protecting information from unauthorized usage. Furthermore, it would have been obvious to one of ordinary skill in the art to allow the forwarded certificate request in de Silva's teaching to include the identifier of the registration authority, and the generated certificate includes said identifier as taught by the modified teaching of Kent better for better protecting information from unauthorized usage.

As to claims 2 and 35, de Silva does not specifically teach the request further includes a second identifier that identifies the principal. However, Kent teaches this matter (column 9 lines 40-47). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the request information in the teaching of de Silva to include a second identifier that identifies the principal because this would allow the system more securely monitoring transactions among the different terminals for better protecting the secrecy of each transaction.

As to claim 4, de Silva teaches authenticating said certificate by said certificate authority (column 4 lines 55-67).

As to claim 5, de Silva teaches authenticating said certificate comprises generating a certificate digitally signed by said certificate authority (column1 lines 48-50 and column 11 lines 34-44).

As to claim 6, De Silva does not specifically teach generating a certificate digitally signed by said certificate authority using a private key of a public private key pair associated with said second node. However, Kent teaches this matter (column 10 lines 40-45). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the certificate in the teaching of de Silva to be signed by

using a private key of a public private key pair associated with said second node because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

As to claim 7, de Silva teaches the certificate includes a time stamp that identifies expiration time (column 4 line 65 – column 5 line 10). Kent teaches using time stamps to auditing trails (column 11 lines 29-47). De Silva modified by Kent does not specifically teach the certificate includes a time stamp that identifies a time associated with the request. It would have been obvious to one of ordinary skill in the art to allow the time stamp in the teaching of de Silva modified by Kent to include a time associated with the request because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 8, de Silva teaches authenticating said request by said registration authority (column 4 lines 41-53).

As to claim 9, de Silva specifically teaches digitally signing the certificate against subsequent tampering (column 1 lines 48-50). De Silva does not explicitly digitally signing said request by said registration authority. However, Kent teaches this matter (column 9 lines 40-53). It would have been obvious to one of ordinary skill in the art to allow the certificate request in de Silva's teaching to be signed by the registration authority as taught by Kent for preventing unauthorized access of the information.

As to claim 10, De Silva does not specifically teach the certificate is digitally signed by using a private key of a public/private key pair associated with said first node. However, Kent teaches this matter (column 9 lines 40-53). It would have been obvious

to one of ordinary skill in the art at the time the invention was made to allow the certificate request in de Silva's teaching to be signed by using a private key of a public/private key pair associated with said registration authority because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the information.

As to claim 11, de Silva teaches the certificate includes a time stamp that is associated with expiration time (column 4 line 65 – column 5 line 10). Kent teaches using time stamps to auditing trails (column 11 lines 29-47). De Silva modified by Kent does not specifically teach the certificate includes a time stamp that is associated with a time and date when said request was received by said certificate authority. It would have been obvious to one of ordinary skill in the art to allow the time stamp in de Silva modified by Kent to include a time and date associated with said request was received by the certificate authority because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 37, de Silva further teaches revoking untrustworthy certificates (column 1 lines 11-15, 55-58 and column 4 line 65 – column 5 line 10).

Claims 17-18, 20, 34 and 36 are rejected for the similar reasons as claims 1, 4 and 11.

5. Claims 3, 19 and 28-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Silva et al., U. S. Patent 6,564,320 in view of Kent, U. S. Patent 6,671,804, and in further view of Vaeth et al., U. S. Patent 6,308,277.

As to claims 3 and 19, the modified method of de Silva and Kent teaches generating a certificate as discussed above. De Silva modified by Kent does not specifically teach said certificate further includes a public key associated with said principal, and said second identifier. However, Vaeth teaches this matter (column 4 lines 34-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow said certificate in the teaching of de Silva modified by Kent further includes a public key associated with said principal, and said second identifier because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

Claims 28 and 30 are rejected for the similar reasons as claims 1-3 as discussed above.

As to claims 29 and 31, de Silva teaches the certificate includes a time stamp that is associated with expiration time (column 4 line 65 – column 5 line 10). Kent teaches using time stamps to auditing trails (column 11 lines 29-47). De Silva modified by Kent does not specifically teach the certificate includes a time stamp that is associated with a time or receipt by said certification authority of said request from said registration authority of said request to issue said certificate. It would have been obvious to one of ordinary skill in the art to allow the time stamp in de Silva modified by Kent to include a time and date associated with a time of receipt by said certification authority of said request from said registration authority of said request to issue said certificate because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 32, de Silva teaches the computer program code includes program code for publishing said certificate (column 4 lines 57-58).

As to claim 33, de Silva teaches the program code for publishing said certificate includes program code for forwarding said certificate to a directory server (column 12 lines 14-19).

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Inquire

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mary Cheung whose telephone number is (571)-272-6705. The examiner can normally be reached on Monday – Thursday from 10:00 AM to 7:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell, can be reached on (571) 272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

The fax phone number for the organization where this application or proceedings is assigned are as follows:

(571) 273-8300 (Official Communications; including After Final Communications labeled "BOX AF")

(571) 273-6705 (Draft Communications)

Mary Cheung
Primary Examiner
Art Unit 3621
May 22, 2006

MARY D. CHEUNG
PRIMARY EXAMINER